What is claimed is:

1. A method for securing transactions using electronic deposits (purses), comprising:

combining a grey lock mark with an electronic deposit (purse) of an IC card;

setting a grey lock mark on the IC card to lock grey the IC card while simultaneously recording a first locking card source by the IC card;

merging a debiting operation and a unlocking grey operation into a one step operation on the IC card; and

resetting the grey lock mark to unlock grey the IC card automatically after successfully completing the debiting operation.

2. The method according to claim 1, further comprising:

storing an encryption key of implementing a debiting operation and implementing a mandatory unlocking grey operation in a computer to make a supplementary debit and implementing a mandatory unlocking grey operation for a locked grey IC card on an on-line card terminal with on-line mode.

3. The method according to claim 1, further comprising:

inserting the IC card to a card terminal;

authenticating both the IC card and the card terminal mutually;

locking grey the IC card by the card terminal;

initiating a consumption; and

after the consumption is complete, debiting from an electronic deposit (purse) on the IC card and unlocking grey the IC card by the card terminal.

4. The method according to claim 3, wherein the step of locking grey the IC card comprises:

creating a first authentication code by the IC card according to the first locking card source and transferring the necessary parameters for creating the first locking card source to the card terminal simultaneously;

creating a second locking card source by the card terminal using the same mechanism as the IC card, and with the second locking card source creating a second authentication code and sending the second authentication code to the IC card by the card terminal;

determining by the IC card whether the first authentication code and the second authentication code are identical, and if they are, locking grey the IC card and sending back a grey lock characterized code, created with the first locking card source and corresponding data, to the card terminal;

wherein said debiting from an electronic deposit (purse) on the IC card and unlocking grey the IC card by the card terminal comprises:

creating a third authentication code by the card terminal according to the second locking card source and necessary parameters for debiting, and sending the third authentication code and corresponding parameters together to the IC card;

creating a fourth authentication code by the IC card with the first locking card source and the corresponding parameters using same mechanism;

determining by the IC card whether the third authentication code and the fourth authentication code are identical, and if they are, debiting from an electronic deposit on the IC card and resetting the grey lock mark simultaneously after debiting successfully.

5. The method according to claim 4, further comprising:

storing the third authentication code needed for debiting, the amount of money of an escape card and the grey lock characterized code together as part of a grey record, and sending the grey record to a central computer by the card terminal;

for an IC card with an incomplete ending transaction and without debiting and unlocking the last time the IC card was used, authenticating the grey lock characterized code by the card terminal the next time the IC card is used, which terminal has stored said grey record, to confirm that the first locking card source of the IC card is same as the second locking card source for calculating the third authentication code in said grey record; and after confirmation, executing the debit and unlocking grey operation.

6. The method according to claim 1, wherein said first locking card source is a procedure encryption key (SESPK), correlating to at least a pseudo random number (ICC) created temporarily by the IC card.

7. The method according to claim 6, wherein said procedure encryption key (SESPK) = 3DES (DPK, DATA), where DPK is a consumption encryption key of the electronic deposit (purse), obtained from a consumption main encryption key (MPK)

based on dispersing an application sequence number of the IC card; and DATA is a specific parameter including a temporarily created pseudo random number (ICC) of said IC card, a transaction sequence number of the electronic deposit (purse) (CTC), and the last two bytes of the card terminal transaction sequence number (TTC).

8. The method according to claim 6, wherein:

locking grey the IC card comprises:

sending a card terminal transaction sequence number (TTC) from the card terminal to the IC card;

getting a pseudo random number (ICC) and an electronic deposit (purse) transaction sequence number (CTC) of the IC card;

creating a first procedure encryption key (SESPK) by the IC card and recording the parameters of this creating step and also creating and recording a grey lock characterized code of this time at the same time;

sending the pseudo random number (ICC) and the electronic deposit (purse) transaction sequence number (CTC) from the IC card to the card terminal, which terminal has stored a consumption main encryption key (MPK) in its security authentication module (PSAM);

deriving the electronic deposit (purse) DPK on the IC card with an application sequence number of the IC card by the security authentication module (PSAM); and

creating a second procedure encryption key (SESPK) by the card terminal using the pseudo random number (ICC), the electronic deposit (purse) transaction sequence number (CTC), and the card terminal transaction sequence number (TTC) using the same mechanism as the IC card; and

wherein said debiting step comprises:

calculating a first authentication code by the card terminal with the second procedure encryption key (SESPK), and at least the debit amount, operation date and time, and sending the first authentication code, the second procedure encryption key (SESPK), and at least the debit amount, operation date and time to the IC card;

calculating a second authentication code by the IC card with the first procedure encryption key (SESPK), using the same data and algorithm;

determining by the IC card whether the first authentication code and the second authentication code are identical, and if they are, then debiting and unlocking,

and if they are not, then incrementing an internal error counter and returning an error code without debiting and unlocking; and

locking the IC card application internally to prevent misuse, when the internal error counter reaches a predetermined number.

9. The method according to claim 1, wherein the step of combining a grey lock mark with an electronic deposit comprises creating a refueling electronic deposit.

10. The method according to claim 9, wherein said refueling electronic deposit further includes the functions of refueling transaction, local unlocking grey transaction and on-line unlocking grey transaction.

11. The method according to claim 9, wherein said refueling electronic deposit further includes the states of pre-refueling, grey lock and unlocked grey.

12. The method according to claim 9, wherein said refueling electronic deposit further includes the commands of INITIALIZE FOR REFUEL, LOCK FOR REFUEL, DEBIT FOR REFUEL, INITIALIZE FOR UNLOCK, DEBIT FOR UNLOCK and GET GREY STATUS, wherein the INITIALIZE FOR REFUEL command is used for refueling consumption transaction initialization, the LOCK FOR REFUEL command is used for making grey lock to refueling electronic deposit (purse), the DEBIT FOR REFUEL command is used for local refueling consumption and unlocking grey simultaneously, the INITIALIZE FOR UNLOCK command is used for on-line unlocking and consumption transaction initialization, the DEBIT FOR UNLOCK command is used for on-line unlocking grey transaction and supplementary debiting refueling consumption simultaneously, and the GET GREY STATUS command is used for reading grey lock state and launching local unlocking grey transaction.